해쉬함수 기반의 효율적인 WWW 사용량 측정 방안

신 원[†] · 이경현[††]

요 약

본 논문에서는 WWW 웹페이지에 대한 기존 매체와의 차별성 및 요구사항에 비추어 WWW 환경을 위해 안전하고 효율적인 웹 페이지의 사용량 및 인기도 측정 방안을 제안한다. 암호 기술을 기반으로 하는 웹 측정 방안은 안전성, 효율성, 정확성, 익명성 등을 제공하므로 기존 광고 측정 방식에 비해 웹 서버의 클라이언트 방문 수 부풀리기, 클라이언트의 웹 측정 과정 방해, 서버 및 클라이언트의 공모 등을 막을 수 있는 장점이 있다.

An Efficient WWW Metering Scheme based on Hash Functions

Weon Shin[†] and Kyung Hyune Rhee[††]

ABSTRACT

In this paper we propose a secure and an efficient metering scheme for measuring the usage and the popularity of web pages. The proposed scheme is based on the cryptographic secure hash functions. Since the metering schemes based on cryptographic technology provides security, efficiency, accuracy and anonymity comparing to the existing metering schemes in WWW, they have the advantages that are secure against attempts by servers who inflate the number of clients and against attempt of collaboration of servers and clients.

1. 서 론

컴퓨터 기술과 네트워크 기술의 발전을 기반으로 빠른 속도로 발전해온 인터넷은 1990년대 초 WWW (World Wide Web)의 등장으로 인하여 개인 생활뿐만 아니라 여러 주요 산업에 엄청난 영향력을 발휘하고 있다. 전 세계의 수많은 네트워크를 하이퍼미디어(Hypermedia)로 묶은 WWW은 인터넷 사용인구의 폭발적인 증가를 가져오게 되었고, 특히 상업화의 급진전에 힘입어 각 기업의 새로운 마케팅 전략에 따른 기업 홍보와 제품 광고의 장으로써 활용되고 최근에는 전자상거래에까지 응용되기 시작하였다. 현재 많은 기업이 이를 목적으로 각자의 웹 페이지를 개설하는 것뿐만 아니라 TV나 신문과 같이 상업적인 광고를 위해 대행자를 두고 일반 사용자들을 끌어들이기 위해 노력하고 있다. 그러나 WWW 환경에서 광고는 일반 상업 광고와는 달리 동작 방식의 능동성으로 인해 사용자의 클라이언트와 광고회사의 서버 사이에서 상호동작이 발생하게 된다. 현재 이러한 상호동작에 대한 체계적이고 안전한 측정 방법의 부재로 인하여 서버 웹 페이지에 대한 인기도 및 사용량 등의 정확한 측정이 어려운 실정이다. 이들 서버는 대부분이 자신들이 제공하는 웹 페이지에 대한 클라이언트의 방문 수를 셈으로써 사용량 및 인기도를 측정하고, 이를 근거로 광고 수입이 책정되고 있다[5]. 그러므로 대부분의 광고회사 웹서버들은 상업적인 목적을 위하여 자신들에게 방문했던 클라이언트보다 더 많은 수의 클라이언트가 방문했다고 주장하려 한다. 또한 최근에는 정확한 측정 과정을 방해하려는 악의적인 클라이언트에 의한 서비스 거부 공격

본 연구는 '98년도 귀뚜라미문화재단 연구비의 지원에 의해 수행되었음
† 부경대학교 대학원 전자계산학과
†† 종신회원, 부경대학교 전자컴퓨터정보통신공학부

(Denial of Service Attack) 등도 등장하고 있는 실정이다.

본 논문에서는 암호 기술을 기반으로 하여 WWW 환경에서의 안전하고 효율적인 사용량이나 인기도 등에 대한 기존의 측정 방안을 살펴본 후 새로운 측정방안을 제안한다. 제안된 측정 방안은 서버의 클라이언트(사용자) 방문 수 부풀리기를 방지하고, 측정 과정을 방해하려는 클라이언트에 대해서도 안전하며 특히 클라이언트 입장에서 효율적이며 다른 통신에 방해가 되지 않고 프라이버시를 보호할 수 있는 장점이 있다.

2장에서는 WWW 측정 방안에 대한 요구사항인 안전성(Security), 정확성(Accuracy), 효율성(Efficiency), 익명성(Anonymity) 등을 살펴보고, 3장에서는 측정 방안의 동작 방식을 살펴본다. 4장에서는 여러 기법을 이용한 측정 방안을 살펴본 후 5장에서 새로운 방안을 제안하고, 마지막으로 6장에서는 측정 방안의 응용 기술 및 사례를 들고 결론을 유도한다.

2. WWW 측정 방안의 요구사항

인터넷의 일상화로 인하여 WWW을 이용한 광고 시장이 최근 급속한 규모로 성장하고 있다. 현 증가 추세대로라면 2005년도에는 그 규모가 수백 억 달러에 이르고 국내에서도 4,500억원에 이를 것이라고 예측하고 있다[2]. 이러한 WWW 광고가 원하는 목적대로 원활하게 이루어지도록 하기 위해서는 광고주 자신들의 WWW 광고에 대한 그 효과를 측정하는 방법이 필수적으로 선행되어야 한다. 현재까지 인터넷 광고는 표준화가 완료되지 않았으므로, 광고주는 전통적인 TV나 신문 매체에서 사용하는 형태의 측정법을 이용하여 WWW 광고에 대한 비용을 책정하게 된다. 따라서 WWW 광고는 안전하고 정확하게 측정될 수 있어야 하고, 측정을 위해 시스템에 많은 무리를 주지 않도록 효율적으로 수행되어야 한다. 또한 부가적으로 클라이언트 사용자의 이동성(Turnover)을 측정할 수 있어야 하고 익명성을 보장해주어야 한다. 일반적으로 WWW 광고는 다음과 같은 요구사항들을 반드시 만족해야 한다.

- 안전성(Security) : 올바른 WWW 광고 측정을 위하여 어떤 서버가 자신에게 방문했다고 주장하는 클라이언트의 수를 조작하는 것이 사실상 불가능해야만 한다. 즉, 서버는 클라이언트의 방문 수를 수학적으로 증명할 수 있어야 한다. 또한 측정을 방해하거나 방문 수를 감소시키려는 악의적인 클라이언트로부터도 보호되어야 한다.
- 정확성(Accuracy) : 객관적이고 과학적인 방법을 통하여 측정 방안의 결과는 가능한 한 정확해야 한다. 서버가 수학적인 방법으로 증명하는 클라이언트의 방문 수에 대하여 허용될 수 있는 작은 오차율만을 가지도록 해야 한다.
- 효율성(Efficiency) : 측정 과정이 포함됨으로 인하여 시스템에 많은 부하를 주거나 다른 통신에 방해가 되지 않도록 통신량은 작아야 하며, 특히 사용자 입장에서 클라이언트의 계산량과 메모리 사용량은 가능한 한 최소이어야 한다.

다음 요구사항들은 선택사항으로 위의 필수 요구사항과 함께 추가적으로 만족한다면 WWW 광고를 확장하여 특수한 목적에서도 사용할 수 있도록 해주는 요구사항들이다.

- 이동성(Turnover) : 서버를 방문했던 과거 어느 시점의 클라이언트와 현재 시점의 클라이언트 사이에 대한 비율을 측정할 수 있어야 한다. 즉, 어느 기간 동안 서버를 방문한 대부분의 클라이언트들이 그 이전에도 서버를 방문했는지 아닌지를 설명할 수 있어야 한다. 이동성을 분석하여 사용자의 성향, 사용 시간대, 이동량 등을 측정할 수 있다.
- 익명성(Anonymity) : 측정 과정의 상호동작에서 클라이언트 사용자의 프라이버시를 침해하지 않도록 익명성을 허용해주어야 한다. 보다 강력하게 요구되는 특성은 같은 클라이언트에 의해 발생하는 서로 다른 방문을 서버가 구분할 수 없도록 하는 비연결성을 제공하는 것이다.
- 표준화(Standardization) : T.Novak과 D.Hoffman[5]은 WWW 측정 과정을 표준화하는 것이 중요하다고 논의하였다. WWW 광고는 아직 표준화가 이루어지지 않은 부분이 많으며, 광고 효과 측정 부분에서는 광고 회사의 측정 기준에 따라 그 결과가 서로 다르게 나올 수 있다. 측정 수단, 사용되는 단위의 통일, 결과보고 형태 등이 이 부분에 속하는데 단순한 광고 효과 측정의 객관성 확

보뿐만 아니라 광고비용 산출, 다른 광고 매체에 대한 비교 등을 제공해주어야 한다.

3. 동작 방식

다른 광고 매체인 TV, 신문, 잡지와 마찬가지로 WWW 광고도 객관적인 인증 데이터가 요구된다. 그러므로 독립적인 제 3의 기관과 같은 감사기관에 의한 인증 데이터는 하나의 광고 매체로써 인식하게 하고 일반적으로 인정받는 데이터로 사용될 수 있다. 따라서 감사기관은 웹사이트가 제시하는 사용자 방문 정보를 기반으로 웹사이트의 측정 과정과 그 결과를 검증하는 절차를 거쳐 정확한 데이터로써 인증하게 하므로 제 3의 기관의 역할은 매우 중요하며, 광고회사의 웹사이트에서 제공되는 데이터에 대해 객관성과 신뢰성을 더해준다.

측정 방안이 동작하는 환경은 클라이언트(C, Client), WWW 광고 서버(S, Server), 감사기관(AA, Audit Agency)으로 구성된다. 보통 사용자의 클라이언트와 WWW 광고를 위한 서버 사이에서 어떠한 상호동작이 이루어지고, 감사기관이 이들 상호동작에서의 측정에 대한 책임을 가진다. 클라이언트와 서버는 서로 신뢰할 필요는 없지만 올바른 측정을 위해서는 감사기관만은 신뢰해야만 한다. 경우에 따라서는 부정한 서버끼리 또는 부정한 서버와 부정한 클라이언트끼리 방문 수를 부풀리기 위한 공모도 존재할 수 있기 때문이다.

기본적으로 측정 시스템은 서버가 받아들이는 클라이언트의 방문 수를 측정한다. "무엇을 방문하는가"하는 것은 WWW 광고에서 사용되는 단순한 한 페이지이거나 동영상, 이미지, 사운드, 텍스트 등 어떤 정보도 될 수 있다. 측정 방식의 동작은 <그림 1>과 같은 일반적인 구조를 가지도록 구성된다.

① 초기화 :

$AA \rightarrow S: f_{AA}(\alpha, S)$

$AA \rightarrow C: f_{AA}(\alpha, C)$

시작 단계에서 단방향으로 단 한번 수행되는 과정으로 감사기관 AA는 임의의 비밀키 α를 선택하고, 각 클라이언트 C와 각 서버 S에 대해 초기화 메시지(α와 수신측 식별의 함수)를 생성하여 안전한 채널을 통하여 전송한다. 이 메시지는 측정결과에 대한 증명 때 사용되므로 각각의 클라이언트와 서버에서 비밀로 유지되어야 한다.
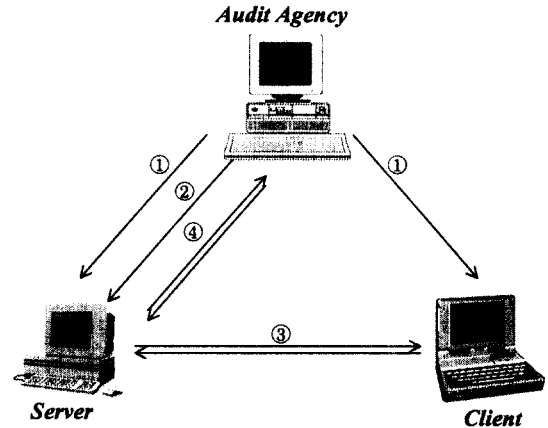
그림 1. 측정 방안의 동작 방식

② 측정 시작 :

$AA \rightarrow S: h_{S,t} = f_{AA}(\alpha, S, t)$

측정 방안의 목적은 어떤 단위 시간 t내에 각 서버를 방문하는 클라이언트의 수를 측정하는 것이다. 어떤 시작 시점에서 AA는 각 S에게 challenge $h_{S,t}$를 생성하여 안전한 채널을 통하여 전송한다. 이 값 역시 비밀로 유지되어야 한다.

③ 상호동작 :

$S \rightarrow C: f_S(h_{S,t}, f_{AA}(\alpha, S), C)$

$C \rightarrow S: f_C(f_S(h_{S,t}, f_{AA}(\alpha, S), C), f_{AA}(\alpha, C))$

C가 S를 방문했을 때, S는 $h_{S,t}$, S의 초기화 메시지, C의 식별자를 인자로 하여 함수값을 계산한 후 C에게 전송하고, C는 받은 값과 자신의 초기화 메시지를 인자로 함수값을 계산하여 이것을 응답으로 S에게 전송한다. 이 응답이 C의 방문에 대한 증거가 되므로 S는 이를 잘 보관하여야 한다.

④ 측정 종료 :

$S \rightarrow AA: f_S(f_C(f_S(h_{S,t}, f_{AA}(\alpha, S), C), f_{AA}(\alpha, C)), f_{AA}(\alpha, S))$

$AA \rightarrow S: h_{S,t} = f_{AA}(\alpha, S, t)$

AA는 t시간 후에 각 S에게 새로운 challenge $h_{S,t}$를 생성하여 안전한 채널을 통하여 전송한다. 이 때 S는 t시간 동안 C에서 받은 응답과 AA에게서 받은 자신의 초기화 메시지를 사용하여 응답함으

로써 자신의 방문 수를 *AA*에게 증명할 수 있다.

위와 같은 측정 방안이 가장 일반적인 형태이다. 여기서 함수 *f*는 감사기관, 서버, 클라이언트에 의해 정의되는 일방향 함수이면 된다. 만약 전송되는 challenge 메시지에 대해 각 수신측에서 직접 계산할 수 있다면 생략하는게 더 바람직하다.

4. 기 제안된 측정 방안

3장에서 언급한 요구사항을 가능한 한 만족하도록 측정 시스템을 단순하게 구현하려면 *AA*가 각 클라이언트에게 인증된 서명키를 제공한 후 클라이언트가 서버를 방문할 때마다 서명하도록 하면, 서버는 방문의 증거로써 클라이언트가 서명한 리스트를 제시함으로써 자신이 주장하는 방문을 증명할 수 있다. 그러나 이 방안은 디지털 서명을 도입함으로써 정확하지만 서명과 그 확인에 따르는 메모리 사용량과 계산량이 매우 비효율적이고 각 클라이언트의 프라이버시를 지킬 수 없다는 단점이 있다.

M.K.Franklin과 D.Malkhi[1]는 "Lightweight Security"만을 제공하여 정확한 방문 수를 측정하는 방안을 제안하였다. 동작 방식은 서버에서 클라이언트 접속시간에 해쉬값을 취한 후 클라이언트에게 전달하고 클라이언트가 사용한 시간 동안 계속해서 해쉬를 취하여 마지막 결과를 서버에게 전달하는 형태로 구성되어 있다. 그러나 이 방안은 방문 수를 조작하기 위해 클라이언트가 서버와 공모하는 것이 가능하고, 서버 단독으로 해쉬값을 생성하여 방문 수를 부풀리는 것도 가능하므로 WWW 광고에 적용하기에는 다소 무리가 있다.

최근 전자상거래가 부상함에 따라 전자화폐의 작업량을 줄이기 위한 효율적인 설계방안으로 "Micropayment"가 새로운 지불방식으로 등장하고 있다[8]. 다양한 지불방식 중 이를 수정하여 WWW 서버 방문 수 측정에 적용할 수 있는데, 방문시 클라이언트가 서버에게 "Money"를 전송하고 서버는 이들 합계가 은행에서 각각 클라이언트에게 발행한 Money의 합계가 서로 일치함을 확인함으로써 방문 수를 증명하는 방식이다. 모든 Micropayment 기반 측정 방안은 서버가 받았던 순서대로 Money를 다시 은행(또는 *AA*)으로 전송해야만 하지만 실제 지불 방식과는 달리 은행의 클라이언트 계좌에서 Money를 공제할 필요가 없기 때문에 보다 효율적으로 구성할 수 있는 장점이 있으나, 단순한 WWW 광고 측정을 목적으로 사용하기에는 시스템 구현이 복잡하고 계산량이 많아진다는 단점도 있다.

Shamir[7]의 k-out-of-n 비밀 분산 방안은 WWW 광고 측정 방안을 위한 많은 요구사항을 만족시킨다. 이를 이용한 측정 방안은 감사기관이 비밀(여기서는 어떤 단위 시간당 방문 수)을 n개의 분할로 나누어 각각을 클라이언트에게 배분한 후 서버를 방문할 때마다 서버에게 하나씩 전송하도록 한다. 서버는 k개의 서로 다른 분할을 얻었을 때 비밀을 재구성 할 수 있고 이를 감사기관에게 증명할 수 있다. 만약 서버가 k-1개 이하의 분할을 가진다면 비밀에 대한 어떠한 정보도 알아낼 수 없다. 그러나 서버와 클라이언트의 공모를 염두에 둔다면 1회만 사용하고 계속해서 갱신하도록 해야하고, 하나의 분할이라도 잘못된 경우 비밀을 복구할 수 없기 때문에 잘못되거나 부정한 분할을 미리 인식할 수 있는 방법이 요구된다.

M.Naor와 B.Pinkas[3,4]는 비밀 분산 방안(Secret Sharing Scheme)을 수정하여 이변수 다항식을 이용한 측정 방안을 제안하였다. 이 방안은 감사기관이 다항식을 생성하여 그 해를 클라이언트들에게 나누어준 후 서버에 접속할 때 전달하여 서버가 다항식의 값을 계산하여 감사기관에게 전달하는 형태로 이루어진다. 클라이언트 측면에서는 작은 계산량이 필요한 다항식을 비밀 분산 기법에 적용하여 안전하고 효율적인 측정에 초점을 두었다. 그러나 이 방안에서는 견고성, 효율성, 익명성을 부가하기 위해서 기본 방안의 새로운 수정이 필요하므로 일반적인 목적의 측정보다는 각각의 요구사항이 필수적인 특수한 환경에서의 측정에 유용하다.

<표 1>은 기 제안된 각각의 측정 방안에 대한 장·단점과 특징을 비교하였다.

5. 제안 방안

5.1 새로운 방안

본 논문에서는 WWW 광고의 여러 요구사항에 가장 적합한 M.Naor와 B.Pinkas의 방안[3,4]에 초점을 맞추어 보다 효율적인 방안을 제안한다. 제안 방안은 일방향 함수만을 사용하여 감사기관과 서버에서의

표 1. 기 제안된 측정 방안의 비교

방안 \ 특징	전자서명 방안	M.K. Franklin과 D.Malkhi의 방안	Micro-payment 방안	M.Naor와 B.Pinkas의 방안
장점	매우 정확	정확한 사용량 측정에 용이	정확하고 익명성 보장	효율적이고 안전
단점	클라이언트 측의 많은 계산량	부풀리기 및 공모 가능	시스템 구현의 복잡, 계산량 증가	실제 적용을 위한 수정
참고사항	실제 적용에는 무리	1대 1의 사용량 측정에 적합	WWW 사용량측정에 적용 가능	특수한 환경에 유용

계산량을 다항식에 기반하는 기 제안된 방안에 비교하여 매우 효율적으로 동작한다.

3장에서 설명했던 측정 방안의 동작 방식에서 ① 초기화 과정과 ② 측정 시작 과정에서 감사기관은 비밀키 α를 선택한 후 각 서버와 클라이언트의 식별자를 이용하여 충돌저항 해쉬함수(H)를 이용하여 해쉬값을 취한다. ③ 상호동작 과정에서는 이 값들을 서버와 클라이언트가 서로 교환한다. ④ 측정 종료 과정에서는 서버가 클라이언트에게서 받았던 값들을 XOR를 취하여 감사기관에게 전달하고 이를 확인한다. 측정 방안의 동작 방식에 비추어 감사기관, 서버, 클라이언트가 주고받는 메시지는 다음과 같다.

① 초기화 :

$AA \rightarrow S: H(\alpha, S)$
$AA \rightarrow C: H(\alpha, C)$

② 측정 시작 :

$AA \rightarrow S: h_{S,t} = H(\alpha, S, t)$

③ 상호동작 :

$S \rightarrow C: H(h_{S,t}, H(\alpha, S), C)$
$C \rightarrow S: H(H(h_{S,t}, H(\alpha, S), C), H(\alpha, C))$

④ 측정 종료 :

$S \rightarrow AA: H(H(H(h_{S,t}, H(\alpha, S), C), H(\alpha, C)), H(\alpha, S))$
$AA \rightarrow S: h_{S,t} = H(\alpha, S, t)$

제안 방안은 이와 같이 매우 단순하게 동작하지만 M.Naor와 B.Pinkas의 방안과 비교하면 <표 2>와 같은 특성을 가진다.

표 2. M.Naor와 B.Pinkas의 방안[3,4]과 제안 방안의 비교

요구사항 \ 방안		M.Naor와 B.Pinkas의 방안	제안방안
안전성		안전한 다항식 생성에 기반	해쉬함수의 안전성에 기반
효율성	감사기관	다항식의 생성과 결과의 확인	해쉬값 생성과 해쉬값의 XOR 확인
	서버	다항식 계산	해쉬값의 XOR 계산
	클라이언트	감사기관에서 받은 값을 서버에 단순히 전달	감사기관에서 받은 값을 서버에 단순히 전달
정확성		매우 정확	매우 정확
이동성		수정 요망	수정 요망
익명성		수정 요망	수정 요망

두 방안 모두 n-out-of-n 비밀 분산 방안 형태이고, M.Naor와 B.Pinkas의 방안은 다항식을 기반으로 하고 제안 방안은 해쉬함수에 기반한다. 예를 들어, 1대의 서버와 1000대의 클라이언트 환경에서 일정한 시점 내에 사용량을 측정한다고 가정하자. M.Naor와 B.Pinkas의 방안에서는 감사기관이 999차의 다항식을 생성하고 그 해를 각각의 클라이언트에게 전송한 후 서버는 상호동작시 이를 받아 Lagrange 보간법을 사용하여 해를 생성하여 다시 감사기관에 전송하고 이를 확인한다. 제안방안에서는 감사기관이 비밀키 α와 클라이언트의 식별자를 해쉬하여 그 값을 각각의 클라이언트에게 전송한 후 서버는 상호동작시 이를 받아 XOR하여 다시 감사기관에게 전송하고 확인한다. 따라서, 제안 방안은 다항식 계산에 드는 보간법 대신 XOR 연산만을 이용하여 감사기관 및 서버에서 매우 효율적으로 연산을 수행할 수 있는 특징을 가진다.

5.2 개선 방안

4장에서 논의했던 방안들과 제안 방안을 개선할 수 있는 요소들을 살펴본다.

첫째로 안전성에 있어 살펴본 바와 같이 측정 방안의 성질에 가장 적당한 방안이 바로 비밀 분산 방안이다. 다항식을 이용한 k-out-of-n 비밀 분산 방안은 클라이언트에 있어 계산량 및 메모리 사용량을 줄여주므로 실제 사용에 적당하다. 그러나 부정한 클라이언트나 잘못된 클라이언트에 의해 하나의 분할이라도 이상이 있다면 비밀을 복구할 수 없기 때문에 이를 미리 대비하는 견고성을 보장해 주어야 하는데, 이것은 자기 인증(Self-Authenticating) 코드, 증명가능한 비밀 분산(Verifiable Secret Sharing), 법 위에서의 다항식 계산을 이용하여 가능하다.

둘째로 효율성을 보다 증가시키는 방법으로는 클라이언트 집단을 같은 성질의 클래스로 분할하여 클라이언트 단위로 측정하는 것이 아니라 클래스 단위로 측정함으로써 가능하다. 이는 감사기관과 클라이언트는 어떤 클래스 집단에 소속됨을 알지만 서버는 이 사실을 모르도록 하여 상호동작시 같은 클래스의 클라이언트들은 모두 같은 값을 서버로 전송하도록 한다. 방문수를 계산할 때에는 하나의 방문이 클래스를 이루는 클라이언트 수와 같도록 하여 계산한다. 예를 들어 5개의 클라이언트가 1개의 클래스에 속한다면 하나의 방문은 서버에 의해 5개의 방문으로 계산된다. 그리고 클래스에 속한 클라이언트의 구성은 서버에게는 비밀로 유지된다.

셋째로 이동성을 허용하는 방법은 서버가 이전에 방문시 클라이언트와의 상호작용에서 받은 값을 모두 저장하여 과거 시점과 현재 시점 사이의 비율을 측정함으로써 가능하다. 클라이언트와 저장된 값을 직접 연결하는 것도 가능하지만 클라이언트의 익명성을 해칠 수도 있으므로 시스템의 용도에 맞추어 적절하게 시스템을 구성한다. 예를 들어, 서버는 과거 어떤 p시점의 클라이언트와의 상호작용에서 받은 해쉬값 $H(H(h_{S,t_p}, H(a, S), C), H(a, C))$을 이미 저장한 후 현재 시점 c에서 해당되는 클라이언트로부터 받은 해쉬값 $H(H(h_{S,t_c}, H(a, S), C), H(a, C))$을 비교하여 그 비율을 측정하면 이동성을 계산할 수 있다.

넷째로 익명성을 허용하는 방법은 일방향 함수의 역을 계산하기 어려운 성질을 이용하여 서버가 어떤 방문과 클라이언트를 서로 연결시킬 수 없도록 한다. 클라이언트가 서버에 방문할 때 자신의 ID를 직접 사용하는 것이 아니라 일방향 함수를 적용한 값을 사용함으로써 서버는 그 역을 알아낼 수 없도록 하여 클라이언트의 익명성을 보장하는 형태로 구성한다. 예를 들어, ③ 상호동작에서 서버는 클라이언트의 신분을 이용하여 $H(h_{S,t}, H(a, S), C)$를 생성하는데, 여기서 ID를 C 대신 일방향 함수를 적용한 $f(C)$를 사용한다면 서버는 클라이언트가 생성한 값과 각 클라이언트를 서로 연결할 수 없게 된다.

6. 결 론

전자상거래의 중심이 되고 있는 WWW 환경에서 최근 상업적인 목적으로 가장 각광받고 있는 분야가 바로 WWW 광고이다. 그러나 현재의 WWW을 이용한 광고는 안전하고 정확한 측정 방법의 부재로 인하여 그 인기도라든지 사용량을 객관적이고 보편적으로 측정하기 어렵다. 이를 해결하기 위한 몇몇 방안들이 제안되었지만 2장에서 살펴본 요구사항을 모두 만족하지는 못하고 있는 실정이다. 본 논문에서는 안전하고 정확한 측정 방안을 구현하기 위하여 필수적인 요구사항인 안전성, 정확성, 효율성, 익명성, 이동성 등에 대하여 논의하였다. 일반적인 WWW 사용량 측정 시스템에서 클라이언트, 서버, 감사기관의 상호동작을 살펴보고, 여러 제안 방안을 비교 검토한 후 보다 효율적이고 안전한 방안을 제안하였다.

이러한 측정 방안들은 인터넷 및 WWW 환경에 있어서 일반 광고와 마찬가지로 보편적인 광고를 위한 시스템에 적용될 수 있으며, 암호 기술과 결합하여 보다 안전하고 보다 견고하게 설계된다면 정확한 WWW 광고 측정을 위한 한 분야로써 자리잡게 될 것이다. 특히, 광고주 입장에서는 정확한 측정 자료를 바탕으로 광고비를 책정할 수 있게 되고 이동성을 이용하여 사용자 집단의 특성, 취향 등을 파악하여 서비스의 차별화를 꾀할 수 있고, 사용자들은 익명성을 통하여 개인의 프라이버시를 보호받으며 안전한 양질의 서비스를 제공받을 수 있을 것으로 예상된다.

마지막으로, WWW 광고를 위하여 적용되는 여러 가지 방안들은 WWW 광고를 전통적인 광고와 마찬가지로 인식하도록 해주는 것은 물론 WWW의 특성을 이용하여 능동적인 사용자의 참여를 유도하는 새로운 광고 매체로서의 가능성을 보여주고 있다. 이를 이용하여 일반적인 WWW 광고 측정 시스템뿐만 아

니라 네트워크 가입자를 위한 한정 광고 시스템, 특정 라이선스에 따르는 소프트웨어나 정보 서비스 등의 응용 분야에 활용할 수 있고, 또한 보안 단계에 따른 계층적인 키분배 방안, 저작권 보호를 위한 디지털 워터마킹 기술들과 결합한다면 새로운 활용 분야도 등장할 수 있을 것으로 예상된다.

참 고 문 헌

[1] M.K.Franklin and D.Malkhi, "Auditable metering with lightweight security", Financial Cryptography '97, 1997

[2] M.Kinsman, "Web advertising 1997 : market analysis and forecast", Cowles/Simba Information, Stanford, Connecticut, May 1997

[3] M.Naor and B.Pinkas, "Secure and Efficient Metering", EUROCRYPT '98, Volume 1403 of Lecture Notes in Computer Science, pp. 576-590. 1998

[4] M.Naor and B.Pinkas, "Secure Accounting and Auditing on the Web", Computer Networks and ISDN Systems, Vol.40, Issues 1-7, pp. 541-550, 1998

[5] T.Novak and D.Hoffman, "New metrics for web media: toward the development of web measurement standards", http://www2000.ogsm.vanderilt.edu/novak/web.standards/webstand.html

[6] J.Pitkow, "In search of reliable usage data on th WWW", 6th International WWW Conference, 1997

[7] A.Shamir, "How to share a secret", Comm. ACM vol.22 no.11, pp.612-613, 1979

[8] 한국전산원, "전자 상거래 환경을 위한 기술 조사 연구", http://ncalib.nca.or.kr/HTML/1996/96070/96070.htm

이 경 현

1982년 2월 경북대학교 사범대학 수학교육과 졸업(이학사)
1985년 2월 한국과학기술원 응용수학과 졸업(이학석사)
1992년 2월 한국과학기술원 수학과 졸업(이학박사)
1985년 2월~1993년 2월 한국 전자 통신 연구소, 선임 연구원
1993년 3월~현재 부경대학교 전임강사, 조교수, 부교수
1995년 7월~1996년 7월 Univ. of Adelaide, 응용수학과, Australia 방문교수
1997년 12월~현재 한국멀티미디어학회 학술이사
관심분야 : 정보 보호, 암호학, 안전성 평가, 멀티미디어 통신, 네트워크 성능 분석

신 원

1996년 2월 부산수산대학교(현 부경대학교) 전자계산학과 졸업(이학사)
1998년 2월 부경대학교 대학원 전자계산학과 석사과정 졸업(이학석사)
2000년 2월 현재 부경대학교 대학원 전자계산학과 박사과정 수료
관심분야 : 네크워크 시큐리티, Web 시큐리티, 암호학 응용